Chapter

7 Technology Transfer, Export Controls, and International Programs Security

Introduction

The US Government (USG) transfers defense articles, services, and training to other governments and international organizations through both its traditional Security Assistance (SA) programs and its more recent Security Cooperation (SC) programs. This chapter focuses on the technology and related sensitive or classified information embedded in the articles and services transferred under both SA and SC programs. This chapter will also address the broad spectrum of international programs security requirements.

As markets for military equipment continue to grow, competition based on leading edge technology has caused a significant increase in economic espionage vice military espionage for US technology. Although economic security has become an important part of American foreign policy, military strength will remain an essential instrument of foreign policy. It is Department of Defense (DOD) policy to treat defense related technology as a valuable and limited national security resource. Which technologies should be controlled and to what extent? First we must understand that the US policy on international trade consists of two seemingly conflicting elements:

- Free trade—the importance of international trade to a strong US defense industrial base
- National security—the need to restrict the export of technology, goods, services, and munitions that would otherwise contribute to the military strength of target countries that affect US national security

Keeping in mind the balance between free trade and national security, it is the responsibility of those who control access to technology to understand the laws, regulations, and directives that guide its transfer. Traditional SA programs are mechanisms through which technology transfer may occur. International armaments cooperation programs with allies and friends are another means of transferring technology, especially through codevelopment, coproduction, and commercially licensed production programs.

Once technology transfer is discussed and the methods used to transfer and control that export are covered, one still needs to know how to transfer technology by approved and secured means. Controlling the level of technology transferred to US allies and friends is a subset of the concept of international programs security (IPS). We start with a definition of an international program and the security of the program.

- An international program is a lawful and authorized government or commercial effort in which there is a contributing or receiving foreign participant and information or technology is transferred from one country to another
- International programs security is the total effort that safeguards information and technology identified as requiring control that is generated by, provided to, or transferred in international programs

This chapter will discuss nine main topics concerning technology transfer and export control policy and international programs security requirements (IPSR):

- Concept of technology transfer and export controls
- Controlled Unclassified Information (CUI)
- Foreign Disclosure and the National Disclosure Policy (NDP) (for classified)
- Export approval and license process
- International visits and assignments
- International transfers
- Role of Defense Security Service (DSS) in international programs
- Foreign government and the North Atlantic Treaty Organization (NATO) information
- Committee on Foreign Investment in the US (CFIUS) and foreign ownership, control, or influence (FOCI)

The Concept of Technology Transfer and Export Controls

Technology transfer is the process of transferring, from an industry in one country to another or between governments themselves, technical information relating to the design, engineering, manufacture, production, and use of goods. To comply with US policy, technology transfer is regulated by a myriad of US government (USG) agencies, and is ultimately controlled through a government-to-government agreement that can take the form of a memorandum of understanding (MOU), general security agreement, letter of offer and acceptance (LOA), export license, or other form agreed to by both governments. The *Security Assistance Management Manual* (SAMM), chapter 3, "Technology Transfer and Disclosure," is a key reference when working with SC that deals with technology transfer. It must be noted that the transfer policies addressed in this chapter are concerned with those that relate to military technologies.

The policy and controls discussed herein do not normally apply to common or "public domain" reference material such as military standards, specifications, handbooks, or commercial counterparts to these documents. US industry representatives can determine if their materiel is within public domain by submitting documents to the Office of the Assistant Secretary of Defense for Public Affairs, Director for Freedom of Information and Security Review.

Department of Defense Policy on Technology Transfer

The primary policy governing the process of technology transfer is contained in DODI 2040.02, *International Transfers of Technology, Goods, and Services*. This instruction institutionalizes technology security responsibilities within DOD. The directive establishes working relationships among the Joint Staff, the services, and the defense agencies. Selected US technology laws and other appropriate DOD and military services directives are listed as references to this chapter.

DODI 2040.02 states:

- Dual-use and defense-related technology shall be treated as valuable national security resources, to be protected and transferred only in pursuit of national security and foreign policy objectives. Those objectives include ensuring that:
  - ◊ Critical US military technological advantages are preserved

- ◊ Transfers which could prove detrimental to US security interests are controlled and limited
- ◊ Proliferation of weapons of mass destruction and their means of delivery are prevented
- ◊ Diversion of defense-related goods to terrorists is prevented

- The sharing of defense technology, properly controlled, is a valuable way to ensure our allies participate with the US in future military operations. In applying export and technology security policies, due recognition will be given to the importance of interoperability with allies and coalition partners and to direct and indirect impacts on the defense industrial base. Consistent with this policy, and in recognition of the importance of international and scientific and technological cooperation, the DOD shall apply export control and other technology security policies and procedures in a way that balances economic and scientific interests with those of national security.

Before we can understand how to control the transfer of technology we must define defense articles. Per the *International Traffic in Arms Regulations* (ITAR), part 120.6, "defense article" means any item or technical data designated in part 121.1. Part 121.1 of the ITAR is the *US Munitions List* (USML). The USML documents articles that have a primarily military utility. So the USML has the "items," but what is "technical data?" Again, per the ITAR, section 120.10:

> Technical Data means, for purposes of this subchapter: (1) Information, other than software as defined in section 120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. (2) Classified information relating to defense articles and defense services.

The ITAR goes on to state:

> (5) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain.

Technology Transfer Mechanisms

Within the context of SC, foreign military sales (FMS) and direct commercial sales (DCS) are normally thought of as the primary means by which technology, goods, services and munitions are transferred; however, as the following list (which is not all inclusive) illustrates, there are many different means for effecting transfers:

- Commercial and government sales
- Scientist, engineer, student, and academic exchanges
- Licensing and other data exchange agreements
- Codevelopment and coproduction agreements
- Commercial proposals and associated business visitors
- Trade fairs, exhibits, and air shows
- Sales to third-party nations
- Multinational corporation transfers

- International programs (such as fusion, space, and high energy)
- International meetings and symposia on advanced technology
- Patents
- Clandestine or illegal acquisition of military or dual-use technology or equipment
- Dissemination of technical reports and technical data, whether published or by oral or visual release
- Dissemination of technical reports under DODD 5400.7, *DOD Freedom of Information Act Program*
- Dummy corporations
- Acquiring an interest in US industry, business, and other organizations

The Basics of International Programs Security

To protect technology that is being transferred, one must understand the legal and national policy basis for DOD's international programs and the principal security considerations prior to pursuing an international program. The three primary documents that form the framework for NDP are the Arms Export Control Act (AECA), Executive Order (E.O.) 13526, and the National Security Decision Memorandum (NSDM) 119. Each of these will be covered in more detail below. The final topic will be a discussion of the government-to-government principle. Information for the remainder of this section comes primarily from the International Programs Security Handbook authorized by the Office of the Deputy Under Secretary of Defense (ODUSD) for Policy Integration & Chief of Staff (PI&CoS), February 1995 (Revised June 2009). An electronic version of the handbook can be found at the link in the list of references to this chapter.

Access and Protection

The conditions and criteria established by the basic laws and policies require that two fundamental decisions be addressed prior to sharing US defense articles with another country or international organization:

1. Access: Access is in the best interest of the US
2. Protection: Articles or information will be afforded the proper protection by the recipient

Legal and Policy Basis for Program Security

The three principal documents that provide the legal and national policy basis for security in most DOD international programs include the:

1. AECA – Arms Export Control Act
2. E.O.13526 – Executive Order 13526
3. NSDM 119 – National Security Decision Memorandum 119

AECA

The AECA governs the export of defense articles and defense services to foreign countries and international organizations and includes both commercial and government programs. It authorizes a list of controlled articles, the USML, which is contained in the ITAR published by the Department of State (DOS) and is available on the internet. (See this chapter's references for link.) The AECA forms the legal basis for the security requirements of most DOD international programs. The AECA states that foreign sales (i.e., access) should be consistent with US foreign policy interests, strengthen the security of the US, and contribute to world peace. The AECA also requires the President to provide Congress assurances that the proposed recipient foreign country or international organization has agreed to certain security conditions regarding the protection of the articles or information. The three security-related conditions that must be satisfied to provide export controlled defense articles and information to a foreign country or international organization are:

- Transfer: The recipient country or organization agrees not to transfer title or possession of the articles or related technical data to anyone who is not an officer, employee or agent of the country or organization without prior USG consent
- Use: The recipient country or organization agrees not to use the articles or related technical data or permit their use for other than the purpose for which they were furnished without prior USG consent
- Protection: The recipient country or organization agrees to maintain security and provide substantially the same degree of security as the USG

Executive Order 13526

Executive Order 13526 establishes the executive branch's classified National Security Information Program. Section 4 of this order states that access may be granted only when required in order to perform or assist in a lawful and authorized governmental function. This is the basis of the need-to-know principle. Further, persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch. The executive order also states that classified information cannot be transferred to a third party without the consent of the originator. It also provides for the protection of foreign government information. The executive order is implemented by *Classified National Security Information*, title 32 of the *Code of Federal Regulations* (CFR), part 2001 and 2003, effective 25 June 2010. The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), publishes the Directive as the final rule pursuant to E.O. 13526 relating to classified national security information. It is also covered under Presidential Directive on safeguarding classified national security information and, within DOD, by DOD 5200.01, *DOD Information Security Program*.

NSDM 119

NSDM 119 provides the basic national policy governing decision-making on the disclosure of classified military information (CMI) to foreign governments and international organizations. NSDM 119 reiterates the basic requirements of the AECA and the E.O. 13526 and emphasizes that classified military information is a national asset and the USG will not share it with a foreign government or international organization (i.e., permit access) unless its release will result in a clearly defined benefit to the US and the recipient government or organization will provide substantially the same degree of protection.

Government-to-Government Principle

Classified information is shared with foreign governments and international organizations based on the government-to-government principle. This principle is defined by two activities relating to international programs. It applies to export and disclosure decisions, and to transfers of classified information and materiel.

1. Decision: In keeping with the AECA, E.O.13526, and NSDM 119, the decision concerns whether the USG will release classified information to another government or international organization.

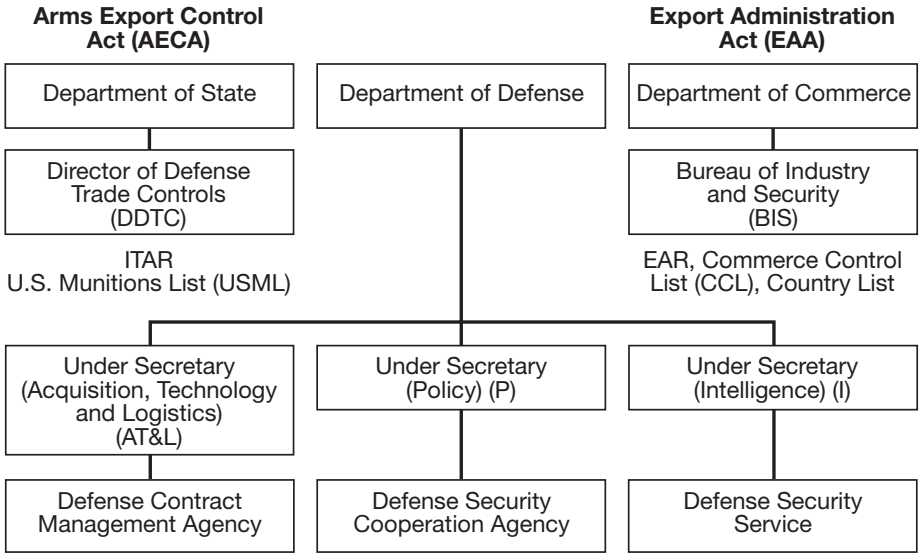
2. Transfer: If the decision above is in the affirmative, the actual transfer must be made either through official government-to-government channels (e.g., government courier) or through other channels approved by the responsible governments.

Transfer via government channels is necessary so that government accountability and control can be maintained from the point-of-origin to the ultimate destination. Transfers normally occur between designated government representatives (DGRs) when custody is officially transferred to the recipient government which then assumes responsibility for the protection of the article or information. A security assurance must be obtained prior to transferring classified material to a representative of a foreign government or international organization and a receipt must be obtained for classified information in material form.

Key Department of Defense Security Organizations

Figure 7-1 provides an overview of the key players within the executive branch for technology transfer and international programs security. The Under Secretary of Defense for Policy [USD (P)] is responsible for international security matters. The Deputy Under Secretary of Defense for Policy Integration & Chief of Staff [DUSD (PI&CoS)] is responsible for day-to-day decisions on NDP. More specifically, the office is responsible for the security policy for international programs. This responsibility includes security policy and arrangements for international programs, international security agreements, the NDP, and NATO security policy. When the DOS or the Department of Commerce (DOC) requires DOD input to decide if a license for export should or should not be approved, the request goes to Defense Technology Security Administration (DTSA). DTSA's responsibilities will be covered in further detail under the topic of "exports" later in this chapter.

Figure 7-1
Key Players in Technology Transfer and International Programs Security



The Under Secretary of Defense for Intelligence [USD(I)] is responsible for DOD counterintelligence, security, intelligence programs, staff supervision of the Defense Security Service (DSS), and for publication of the *National Industrial Security Program Operating Manual* (NISPOM). All of these responsibilities, including security support for program protection planning, have applications to DOD acquisition programs. With the DSS field offices, USD(I) ensures that companies that manufacture military items adhere to the same laws and regulations concerning technology transfer as do individuals working for the USG.

The Under Secretary of Defense for Acquisition, Technology and Logistics [USD (AT&L)] is responsible for Defense Procurement and International Armaments Cooperation Programs (IACP). These functions are performed by the Director, Defense Procurement and the Director, International Cooperation. The Defense Contract Management Agency (DCMA) also reports to USD (AT&L). In addition to its normal management of DOD contracts, DCMA provides industrial security support at those defense contractor facilities where a DSS representative is not available.

The Joint Staff provides support that includes conducting operational and military mission impact assessments on technology, goods, services, and munitions transfer issues, as requested.

The Defense Intelligence Agency (DIA) performs the following functions in the support of US defense technology security:

- Provides assessments of the types and numbers of illegal transfers of technology, goods, services, and munitions, and the associated transfer mechanisms.
- Designates a point of contact to represent DIA on technology transfer matters.
- Conducts end user checks and intelligence review on technology, goods, services, and munitions transfer cases.
- Assesses foreign availability of technology, goods, services, and munitions proposed for transfer.
- Provides intelligence concerning the total effect of transfers of technology, goods, services, and munitions on US security.
- Provides intelligence expertise in interagency, national, and international fora on technology, goods, services, and munitions transfer matters.
- Assists in identifying and assessing critical technologies.

The DOD export control responsibilities and participating organizations are further depicted in table 7-1.

Table 7-1
Department of Defense Organizational Export Control Responsibilities

Organization	Responsibility
USD (AT&L)	Technical oversight for national security and nonproliferation
	Vice Chairman International Technology Transfer
	Coordinating Committee (ITTCC)
	National Economic Council representative
	Economic security balance
USD (P)	Policy oversight
Joint Staff	Strategic rationale and validation
Intelligence community	Threat assessments of foreign nations
Military departments	Provide experts from defense labs and commands
Institute for Defense Analysis	Federally-funded R&D center providing USD (AT&L) with technical support and economic security assessments
Industry and academia	Participate in technical working groups and multilateral negotiation

Exports through the Department of Commerce

Under the Export Administration Act of 1979 (EAA), the DOC has licensing jurisdiction over all commodities and unclassified technical data except for certain specified items handled by other government agencies, such as USML items by the DOS, or atomic energy material by the US Department of Energy. The EAA applies to the following:

- Exports of commodities and technical data from the US
- Re-exports of US-origin commodities and technical data from foreign destinations
- US-origin parts and components used in a foreign country to manufacture a foreign end product for export and in some instances, a foreign product produced as a direct product of US-origin technical data

The *Export Administration Regulations* (EAR) (15 CFR Parts 368 through 399) issued by the DOC, Bureau of Industry and Security (BIS), prescribe licensing procedures for items under its jurisdiction. Controls on the issue of export licenses are based on considerations of national security, the fostering of US policy and international responsibilities, the necessity for protecting the domestic economy from an excessive drain of scarce materials, and the reduction of the serious inflationary impact of abnormal foreign demand. The DOC and BIS home page is at http://www.bis.doc.gov.

Items controlled by the DOC for export are listed on the *Commerce Control List* (CCL). The list is very detailed and lists items that may be exported to a certain country.

Dual-use items are items that were designed with no intrinsic military function but which may have a potential military application (i.e., computers, jeeps, trucks, light aircraft, and global positioning systems). The DOC is charged with coordinating export requests for such items that fall into this category of dual-use. However, once a dual-use item is modified for specific military use, the export will be controlled by DOS. The DOS, DOD, and DOC resolve the commodity jurisdiction issues, and the DOS notifies DOD and DOC that the article falls under the DOS control and is listed on the USML.

Exports through the Department of State

Section 38, AECA, authorizes the President to control the import and export of defense articles and services, to designate such items as constituting the USML, and promulgate implementing regulations. By E.O. 11958, the President has delegated his responsibilities to the Secretary of State, except that the designation of items as defense articles and services for export control requires the concurrence of the Secretary of Defense. Those responsibilities related to the control or regulation of imports of defense articles and defense services are delegated to the Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives except that designation of items as defense articles and services for import control require concurrence of the Secretaries of State and Defense.

The ITAR, 22 CFR parts 120-130, implements the AECA statutory authority to control the export and import of defense articles and services. By virtue of delegations of authority by the Secretary of State, these regulations are primarily administered by the Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs, DOS.

DDTC is responsible for issuing export licenses for those items on the USML. The USML can be found in section 121.1 of the ITAR and is also discussed in SAMM, C4.3. While not a list of specific items (e.g., M-16, M-1A1, F-16, F-18, etc.), the USML generically designates articles, services, and related technical data as defense articles and defense services in accordance with section 38, AECA. Those defense articles preceded by an asterisk (*) on the USML are designated significant military equipment (SME) that section 120.7 of the ITAR defines as, "articles for which special export controls are warranted because of their capacity for substantial military utility or capability." Any classified article or information is always considered SME.

The DDTC processed approximately 65,000 defense-related license requests in FY 2011 from US contractors. Approximately 20 percent of these are forwarded to DTSA and the military departments (MILDEPs) for further review. The DOS regulates permanent exports, temporary exports, and temporary imports of defense articles into the US, and the Department of Justice regulates permanent imports of defense articles (22 CFR parts 47, 178, and 179).

The USML is divided into twenty-one categories. An example would be Category VII –Tanks and Military Vehicles. The categories are further divided into subtypes like, Cat VII *(b) "Military tanks, combat engineer vehicles, bridge launching vehicles, half-tracks and gun carriers." (Note: the (*) before the (b) denotes everything listed in this subtype is SME.) Officials in foreign governments have stated for many years that such broad lists require export licenses for everything dealing with the major item on the list. Example, since "engineer vehicles" are listed, why must the tires for the vehicles be considered USML items? The task of transferring items from the USML to the CCL started under the Bush Administration and continues under the Obama Administration. Cat VII is the first category to be reviewed. The goal is to eventually have just one list with only the truly key defense materiel listed as controlled. This process will take many years, but at least it has started.

Controlled Unclassified Information

Controlled unclassified information (CUI) is a DOD term used to describe collectively all unclassified information to which access or distribution limitations have been applied in accordance with applicable national laws or regulations. For the US, CUI is official government information that is unclassified, but that has been determined by designated officials to be exempt from public disclosure under the Freedom of Information Act (FOIA), which is designed to make government information available to the public and thus requires openness in government. It is not designed to protect information. It provides that the public is entitled to access to agency records, unless the record is exempt from disclosure. There is no executive order to implement FOIA. Government agencies apply their own unique markings to identify the information. Consequently DOD has several policy directives covering the disclosure of official information. These documents are listed as references to this chapter.

- DODD 5230.09 contains policies and procedures for the release of information for publication or public release.
- DODI 5200.21, DODD 5230.24, and DODD 5230.25 govern the release of DOD technical information.
- DOD 5400.7-R contains the DOD policies and procedures governing FOIA requests.
- Official information that meets the standards for security classification is classified and protected in compliance with E.O. 12958 and DOD 5200.01.
- DODD 5230.25 provides procedures for the dissemination and withholding of unclassified technical data.

On 9 May 2008, President Bush signed the Memorandum For The Heads Of Executive Departments And Agencies on the subject of "Designation and Sharing of Controlled Unclassified Information (CUI)." Implementation of these new procedures is scheduled to take up to five years. The memorandum states the following:

> . . . adopts, defines, and institutes "Controlled Unclassified Information" (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as "Sensitive But Unclassified" (SBU) in the Information Sharing Environment (ISE), and establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI.

On 27 May 2009, President Obama signed the Memorandum for the Heads of Executive Departments and Agencies with a subject of "Classified Information and Controlled Unclassified Information." In it, President Obama states:

> [M]y Administration is committed to operating with an unprecedented level of openness. While the Government must be able to prevent the public disclosure of information where such disclosure would compromise the privacy of American citizens, national security, or other legitimate interests, a democratic government accountable to the people must be as transparent as possible and must not withhold information for self-serving reasons or simply to avoid embarrassment.

This initiative may result in major changes as to how CUI is handled and disseminated. It will take years to implement all the changes, but US officials dealing with foreign counterparts must be aware of the evolution of these policy changes.

Freedom of Information Act

Congress has stated the US public generally has the right to know what its government is doing. FOIA requires government information to be made available to the public unless the information falls within one of nine exemption categories described and the appropriate USG official determines the information should be withheld from disclosure.

- Exemption 1 is classified information. The FOIA permits the withholding of any information properly and lawfully classified under the provisions of E.O. 13526. The other eight exemption categories deal with unclassified but generally sensitive information.
- Exemption 2 permits the withholding of information which pertains solely to the internal rules and practices of a government agency.

- Exemption 3 permits the withholding of information that a statute specifically exempts from disclosure by terms that permit no discretion on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld.
- Exemption 4 permits withholding information such as trade secrets and commercial and financial information obtained from a company on a privileged or confidential basis which, if released, would result in competitive harm to the company.
- Exemption 5 protects inter- and intra-agency memoranda which are deliberative in nature.
- Exemption 6 provides for the withholding of information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of personal privacy of individuals.
- Exemption 7 permits withholding records or information compiled for law enforcement purposes that could reasonably be expected to interfere with law enforcement proceedings; would deprive a person of the right to a fair trial or impartial adjudication; could reasonably be expected to constitute an unwarranted invasion of personal privacy of others; disclose the identity of a confidential source; disclose investigative techniques; or could reasonably be expected to endanger the life or physical safety of any individual.
- Exemption 8 permits withholding records or information contained in or relating to examination, operation or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions.
- Exemption 9 permits withholding records or information containing geological and geophysical information and data (including maps) concerning wells.

It is DOD policy to place distribution statements on documents containing unclassified scientific and technical information produced either within DOD or on its behalf by others. This policy was only marginally directed toward restricting the disclosure of such information to the public and thus to foreign persons. Moreover, although it was the policy to apply such distribution markings, the practice did not always conform to the policy. The result was that sensitive scientific and technical information occasionally found its way into the public domain, including the foreign public. This potential loophole was resolved by Public Law 98-94, enacted 24 September 1983, which provided the Secretary of Defense with the authority to withhold from the public critical technologies under Exemption 3 of the FOIA. For more specific information on FOIA as it relates to LOAs and FMS procurement contracts, refer to SAMM, section C3.4, "Release of Information."

Foreign Disclosure and the National Disclosure Policy

The NDP was established as framework for the approval or denial of the transfer of classified military information (CMI) to foreign governments and international organizations. CMI is defined as classified information that has been developed by or for the DOD, or is under the DOD's jurisdiction or control. Basic authority and policy for transferring classified information are contained in NSDM 119, which is implemented by the classified publication, *National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations*, short title NDP-1.

Effective implementation of NDP-1 is the responsibility of the Under Secretary of Defense for Policy [USD (P)]. Disclosure officials are authorized, but not automatically obliged, to disclose information up to the classification levels indicated in the NDP-1 annex for each category of information. And most importantly, each disclosure decision is made on a case-by-case basis.

National Disclosure Policy Committee/Exceptions to National Disclosure Policy

The NSDM 119 and DODD 5230.11 *Disclosure of Classified Military Information to Foreign Governments and International Organizations* requires the establishment of an interagency National Disclosure Policy Committee (NDPC), to formulate, administer, and monitor NDP. General members of the NDPC include:

- Secretary of State
- Secretary of Defense (Chairman)
- Secretary of the Army
- Secretary of the Navy
- Secretary of the Air Force
- Chairman, Joint Staff

On a day-to-day basis, these officials are represented in NDPC decisions by designated senior officials on their staff. NDPC general members have a broad interest in all committee activities and vote on all issues that come before the committee. Other members (such as the director of national intelligence, the secretary of energy, and many others) may vote on issues in which they have a direct interest. See attachment 7-2 for a list of all the members of the NDPC. When an exception to NDP (E-NDP) is required, because disclosure criteria cannot be met within the existing authorized classification level, such exceptions can be granted only by the NDPC, the Secretary of Defense, or the Deputy Secretary of Defense. A request for an E-NDP must be sponsored by a NDPC member, normally the cognizant MILDEP for the classified information proposed for transfer. For military weapon systems, this is normally the MILDEP which has developed and produced the system.

The NDP-1 annex (classified) identifies the maximum classification level of information that can be released by country and by category of classified military information. NDP-1, by itself, does not authorize any disclosures. The secretaries of the military departments have generally been delegated authority by the NDP-1 to decide if CMI under their control can be released. The policy and guidance for implementing NDP-1 is contained in the DODD 5230.11. This directive states that the MILDEPs will release CMI in accordance with the NDP-1 annex only if all of the following five conditions or criteria, originally outlined in NSDM 119, are met:

1. Disclosure is consistent with US foreign policy and national security objectives
2. Disclosures, if compromised, will not constitute an unreasonable risk to the US position in military technology or operational capabilities
3. The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the US. The intent of a foreign government to protect US CMI is established in part by the negotiation of a general security of military information agreement (GSOMIA) or other similar international agreement
4. Disclosure will result in benefits to the US at least equivalent to the value of the information disclosed
5. The disclosure is limited to information necessary to accomplish the purpose for which disclosure was authorized

If the classification of the information proposed for disclosure exceeds the country's eligibility in the NDP-1 annex, or if the policy criteria cannot be met, then the proposed disclosure must be denied or an E-NDP must be approved by the NDPC. Moreover, even if the US disclosure official has determined that eligibility in the NDP-1 annex exists and that all policy criteria have been met, disclosures of classified military information may not be made until the affected originator's approval has been obtained or appropriate authority to disclose has been received.

All disclosure authority rests in the first instance with the head of the department or agency which originates the information. In addition, all disclosure officials must be certain that they possess the required authority to disclose the information in question. The Secretary of Defense and the Deputy Secretary of Defense are the only officials who may grant unilateral exceptions to the NDP. Under DOD Directive 5230.11, the Secretary of Defense has delegated disclosure authority to the secretaries of the MILDEPs and other DOD officials whose decisions must be in compliance with NDP-1. They are required to appoint a principal disclosure authority at component headquarters level to oversee the disclosure process and a designated disclosure authority at subordinate commands. SAMM, section C3.5, "Disclosure of Classified Military Information," provides additional information on the national disclosure process as it relates to SC.

Security Surveys

In addition to making determinations on the release of CMI, the NDPC also conducts security surveys (also called security visits) of partner nations. NDPC teams conduct periodic visits to foreign governments and their national industrial bases to assess their capability and intent to protect US-origin CMI. The teams are usually made up of members of the DOS and DOD. The primary areas reviewed by the teams are personnel security, information security, and physical security. The views of the local US embassy are also sought. If the result of a survey is satisfactory, it may result in an international security agreement (see below) with the other government. A survey may also result in changes to the classified annex in NDP-1 concerning a country's classification and eligibility for CMI without engaging the E-NDP process.

International Security Agreements

Before classified information is released outside the executive branch of the USG, E.O. 13526 requires that written assurances must be obtained that the information will be afforded proper protection. In situations where classified information is being made available to foreign governments, these assurances may be obtained in several ways. First, they are included in the standard terms and conditions of FMS LOA, section 2, "Conditions–General Purchaser Agreements." See chapter 8 of this textbook, "Foreign Military Sales Contractual Agreements," for further information. They may also be the subject of diplomatic notes, memoranda of understanding and similar correspondence. Separate international agreements known as General Security of Military Information Agreements (GSOMIAs) have been concluded with over sixty countries. Since these are reciprocal agreements, the other governments may also send teams to the US to ensure compliance with the agreements. GSOMIAs typically include the following topics:

- Protection, third-party transfer, and intellectual property rights provisions
- Classified information transfer mechanism (government-to-government)
- Definition of classified information
- Reciprocal provision for security expert visits
- Requirements for investigations in case of compromise

- Industrial security procedures
- Visit request procedures
- Limitations on level of classification

Disclosure Planning

DOD Directive 5230.11 requires that planning for possible foreign involvement should start at the beginning of the weapon system acquisition process to facilitate decisions on disclosure in support of foreign sales or cooperative programs. Chapter 13 of this textbook, "Systems Acquisition and International Armaments Cooperation," contains additional information.

Technology Security and Foreign Disclosure (TS&FD) Review Processes

In January 2010, the Export Control Reform Task Force (ECR TF) issued a report in response to Presidential Study Directive 8 (PSD 8). The report found that the existing DOD-led TS&FD review processes have many strengths and have served DOD well for many years. However, these processes need to be harmonized and streamlined to better serve DOD, our international partners, and national security strategy. The ECR TF ultimately recommended initiation of an effort "to streamline and harmonize" USG TS&FD processes.

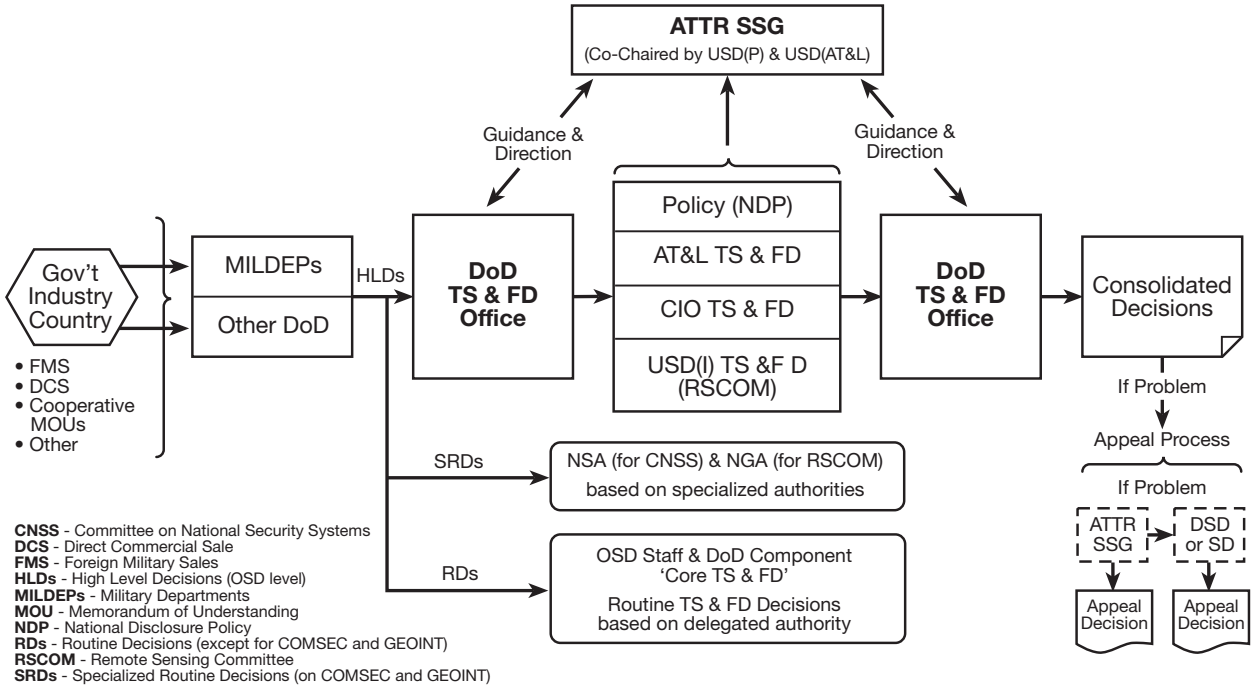
There are thirteen separate but related TS&FD processes that support DOD TS&FD release decisions. Additionally, each of the Military Departments has its own internal review processes for determining the transfer of capabilities and technologies within their purview.

In response to the recommendations outlined in PSD 8, the Deputy Secretary of Defense has further empowered the Arms Transfer and Technology Release Senior Steering Group (ATTR SSG) as the primary forum for review and adjudication of High Level Decisions (HLDs) TS&FD release requests. It also established a Technology Security and Foreign Disclosure Office (TSFDO) as the ATTR SSG's Executive Secretariat. The ATTR SSG has been charged with streamlining and harmonizing DOD TS&FD release processes. The ATTR SSG shall develop, guide, and direct, consistent with U.S policy and national security objectives, DOD-wide reform, implementation, and subsequent management of, the DOD TS&FD system to ensure critical US technologies are protected and release considerations are balanced with building allied and partner nation capability objectives.

The TSFDO will facilitate the coordination and synchronization of release requests through the TS&FD processes to provide transparency and timely and well-informed HLDs. (See figure 7-2). Among its many functions, the TSFDO will consult with TS&FD authorities in assessing and recommending changes to the existing TS&FD policies and processes; develop and implement procedures and checklists that provide guidance to the DOD TS&FD community on submission formats for TS&FD HLD requests; and, conduct screening, triage, staffing and tracking functions for ATTR SSG HLDs.

At the core of this initiative is the establishment of policy and responsibilities for the reform of TS&FD processes to minimizing process complexities; ensuring timeliness and efficient processing of TS&FD release review requests; and implementing holistic DOD-wide TS&FD release review procedures. Ultimately, these reforms will foster Defense industrial base growth, reduce the stress on US forces and facilitate efforts in training and equipping forces in countries where doing so advances US national security interests.

Figure 7-2
DOD TS & FD System



False Impressions

It is the policy of the US to avoid creating false impressions of its intention to provide classified military material, technology, or information. Lack of strict adherence to this policy may create problems. Much military hardware is unclassified; however, this same unclassified hardware, if sold, may require the release of classified information for its operation or maintenance, or for the foreign recipient training. Therefore, the disclosure decision must be made based on the classification level of all information which may be required for release if the system were to be acquired. If the proposed foreign recipient is not authorized to receive the highest level of classified information required, no information, not even CUI, may be released or discussed until the required authority is obtained. This means that there can be no weapon specific information, and no release of FMS price and availability (P&A) data until authority is obtained to release the highest level of classified information ultimately required for disclosure.

In order to avoid false impressions, designated disclosure authorities must authorize in advance any proposals to be made to foreign governments that could lead to disclosure of classified military information, technology, or materiel.

Export Approval and License Process

Before discussing the approval and license process for the authorized export of a military article or service we first must define the term "export." To paraphrase the ITAR section 120.17, an export is sending or taking defense articles out of the US in any way. This includes transferring registration, ownership, or control of an item on the USML to a foreign person. It also includes disclosing orally or visually any defense article to a foreign person in the US or abroad. That means that if you discuss US military technology anywhere with a foreign person that does not have a need to know the information and you do not have an authorization to do so, this is an illegal transfer. Part 127 of the ITAR covers violations and penalties of unlawful export, re-export or retransfer or attempt to retransfer of any defense article or technical data for which a license or written approval is required from the DOS.

Licenses for the Export of Defense Articles

Parts 123 and 125 of the ITAR provide the licensing requirements for the export or temporary import of defense articles or services into or out of the US Any person who intends to export or to import temporarily a defense article or services must obtain the approval of the State Department's Directorate of Defense Trade Controls (PM/DDTC) prior to the action unless there is a regulatory exemption.

Section 123.10 provides for the Form DSP-83 to certify the non-transfer and use assurance certificate required for the export of SME, classified articles, and technical data. A license will not be issued until a completed Form DSP-83 has been received by DDTC. The form is to be executed by the foreign consignee, the foreign end-user, and the applicant. Application for export license for the export or import of classified defense articles and services must be made on DOS Form DSP-85. (See SAMM, figure C3.F3) Application must be made by a US national in accordance with the provisions of sections 125.3, 125.7, and 125.9 of the ITAR.

Table 7-2 provides a guide as to which form is required for the export of munitions list items through either FMS or direct commercial sale. The acronym DSP stands for Department of State Publication. DSPs 5, 61, 73, and 85, when approved, constitute a license.

Table 7-2
Forms to be Used for Export/Import of United States Munitions List Items

Activity	Foreign Military Sales	Commercial Sales
Registration Statement	N/A for gov't shipment	DS-2032
Permanent export of unclassified defense articles and related unclassified technical data	LOA and DSP-94	DSP-5
Permanent/temporary export or temporary import of classified defense articles and related classified technical data	DSP-85 and DSP-94	DSP-85 (with DSP-83)
Temporary export of unclassified defense articles	DSP-73	DSP-73
Temporary import of unclassified defense articles	DSP-61	DSP-61
Non-transfer and use assurances for export of defense articles and services	N/A (Already included in LOA)	DSP-83
Shipper's export declaration	Department of Commerce Form 7525-V	Department of Commerce Form 7525-V

Export License Applications Staffing within Department of Defense

As stated earlier in this chapter when covering government organizations, the License Directorate of DTSA is the DOD entry point for export requests from the DOS and DOC. It is the technical responsibility of this directorate's staff to ensure that the MILDEPs, appropriate DOD agencies, and the technical staff of the USD (AT&L) review applicable export requests or munitions cases. To expedite the licensing process, the DOS delivers these cases for concurrent review by those military services and DOD agencies and components which the DOS believes have an interest in the cases.

After receiving recommendations from the DOD review, the DTSA License Directorate develops the DOD position in concert with DTSA technical and policy staffs, and forwards the position to the

DOS. Most differences within DOD are resolved at the working level. Those that cannot be resolved are referred to DTSA's International Technology Transfer Panel (ITTP) for resolution.

Foreign Military Sales License Exemption

To paraphrase section 126.6(c) of the ITAR, when using the FMS program a license from the DOS is not required if the defense article or technical data or a defense service to be transferred was sold, leased or loaned by the DOD to a foreign country or international organization using the LOA as authorization. In other words, the entire FMS program of DOD operates under a licensing exemption authorized by the ITAR. The actual documents required to use this exemption are the DSP-94 and a copy of the LOA. The ITAR part 126.6(c)(6)(ii) specifically states, "At the time of shipment, the Port Director of US Customs and Border Protection is provided an original and properly executed DSP-94 accompanied by a copy of the LOA and any other documents required by US Customs and Boarder Protection in carrying out its responsibilities."

Commercial Agreements Requiring Approval by Department of State

Besides normal export licenses, when approved by DDTC, the ITAR provides for commercial agreements that give authorization to export certain types of technical information and services. These differ from normal export licenses in that they are broader in scope, more flexible, and remain in effect for longer periods of time. These agreements are typically for ongoing projects rather than a one-time export. The ITAR recognizes three categories of such agreements:

- Technical assistance agreement (TAA). An agreement for the performance of defense services or the disclosure of technical data, as opposed to an agreement granting right of license to manufacture defense articles. [22 CFR 120.22]
- Manufacturing licensing agreement (MLA). An agreement whereby a US person grants a foreign person an authorization or a license to manufacture defense articles abroad and which involves or contemplates the export of technical data or defense articles or the performance of defense services or the use by the foreign person of technical data or defense articles previously exported by the US person. [22 CFR 120.21]
- Distribution agreement. A contract between a US person and a foreign person to export unclassified defense articles to a warehouse or distribution point outside the US for subsequent resale. These agreements contain conditions for special distribution, end-use and reporting. [22 CFR 120.23]

The use of the term person means a natural person as well as a corporation, business association, partnership, society, trust or any other entity, organization or group, including governmental entities. [22 CFR 120.14]

As a review, there are three authorized methods to export USML items to a foreign government or international organizations.

1. A license, i.e. DSP-5
2. An agreement, i.e. TAA
3. An exemption from needing a license, i.e. ITAR 126.6(c), FMS use of an LOA and DSP-94

International Visits and Assignments

International Visits Program

DODD 5230.20, *Visits and Assignments of Foreign Nationals*, sets forth standard procedures concerning requests for visits, certification of liaison officers and personnel exchange programs. SAMM, section C3.5.5, "Visits, Assignments and Exchange of Foreign Nationals," provides further discussion relating to SC.

Foreign representatives, i.e., foreign nationals or US citizens or nationals who are acting as representatives of a foreign government, firm, or person, may be authorized to visit DOD components or US defense contractor facilities only when the proposed visit is in support of an actual or potential USG program (e.g., FMS, USG contract, or international agreement). The DOD and US defense contractors receive over 230,000 foreign visitors annually on matters related to mutual security and cooperation. These visits play a vital part in the exchange of information and technology as a part of US international commitments. These visits account for more transfer of CMI and CUI than all other transfer mechanisms combined.

The International Visits Program (IVP) establishes policy and procedures to control international visits and the information to be transferred during those visits. DOD policies and procedures pertaining to foreign visits are designed to achieve three objectives.

- Facilitate planning, scheduling, and administration of a visit
- Provide a vehicle for consideration of proposed export/disclosure decisions related to the visit and record the decision(s)
- Obtain the required assurances regarding the security clearance, need-to-know, and sponsorship from the visitor's government if classified military information is involved

Types of Visits

Under the IVP, there are three types of visits that may be authorized:

- A one-time visit (normally less than thirty days)
- For recurring contacts for a period of time, normally not exceeding one year
- For an extended period of time, e.g., certifications of liaison officers, normally up to one year or term of contract or applicable export license

In an emergency, a one-time visit may be submitted for approval less than twenty-one working days before the visit start date. Emergency visits may only be authorized if failure to make the visit would jeopardize performance on a contract or program, or cause the loss of a contract opportunity. These authorities may not be used to employ foreign nationals.

A visit can be considered a hosted visit when a DOD official or entity extends an invitation to a foreign national or delegation. Whether DOD funds any portion of the visit is an entirely separate issue from the approval of the visit under the IVP. Before issuing an invitation, DOD officials must ensure that any classified information proposed for disclosure is approved by the delegated disclosure authority. DOD officials who wish to invite foreign representatives to visit a DOD component, or who wish to have a foreign national certified to the component, shall coordinate their actions with DIA or the MILDEP concerned before extending an invitation. Amendments to visits may be used only to change dates (no earlier dates) and list of visitors. The information to be discussed during the visit cannot change.

Visit Procedures

The DIA coordinates the IVP for DOD. Visit requests to DOD organizations or facilities are submitted by the foreign embassy in Washington DC, usually by a military attaché of the partner nation. The requests normally are submitted electronically through the automated Foreign Visit System (FVS) which has been provided by DIA to foreign embassies. The FVS is a component of the Security Policy Automation Network (SPAN). Requests by foreign embassies shall normally be submitted at least thirty days in advance for visits and ninety days in advance for liaison officer certifications.

The FVS automatically routes each request for visit to the Defense Visit Office (DVO) in one of four designated organizations. These include the Department of the Army, Department of the Navy, and Department of the Air Force for all organizations, facilities, and other entities under their control. The fourth organization is DIA itself, which administers visit requests for the Office of the Secretary of Defense, the Joint Staff, defense agencies, and their contractors. The DVOs forward, as necessary, the visit requests to the appropriate foreign disclosure offices of the organizations to be visited, and seek their comment. Based on this input, the DVO renders a decision on the visit which is returned over the same electronic path used for submission to the embassy of the country submitting the visit request. There are three possible responses to a visit request through IVP channels:

- Approved. The visit can occur and the specified information can be disclosed.
- Denied. The visit can occur but the specified information cannot be disclosed.
- Not sponsored. There is no apparent government program. The visit can occur and information can be disclosed if there is a license or other authorization.

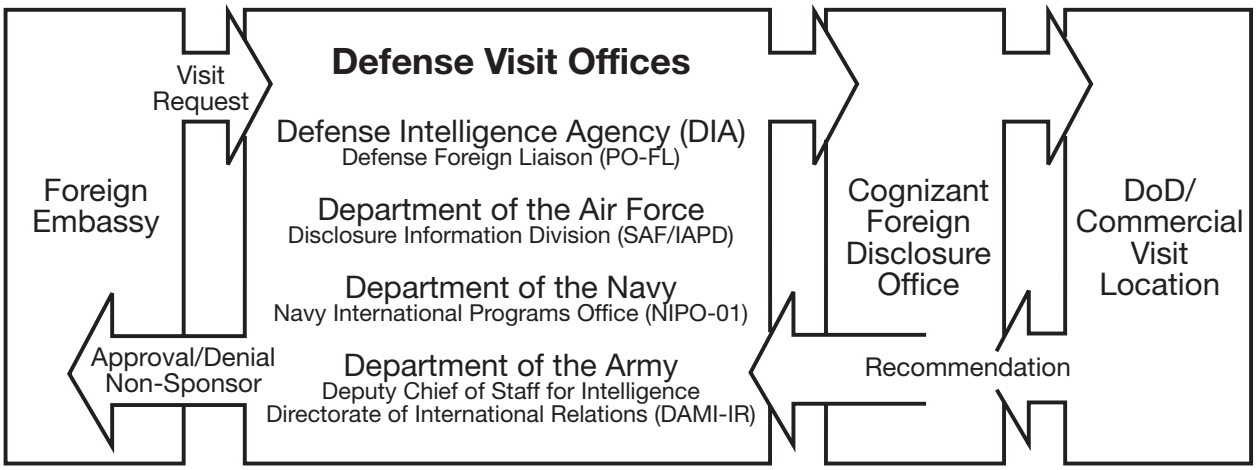
An international agreement is also necessary for personnel exchange programs and on-site assignments of liaison officers. Correspondence with DOD contractors relative to approved foreign visits shall be forwarded to the cognizant DSS regional office for transmittal to the contractor.

Notification of approval of a foreign request for a visit or certification to a DOD component shall be forwarded to the contact officer of the DOD component concerned, or where the representative will visit. This notification shall contain adequate guidance regarding the parameters of the subject visit and the maximum permissible level of classified information that has been authorized for disclosure.

Disclosures of classified information to foreign visitors and certified foreign representatives shall be limited to releasable oral and visual information, unless the release of documentary information is specifically authorized in an approved visit request or letter of acceptance for certified officials, or when the US contractor has secured an export license specific to the documentation intended for release. When documentary release is authorized, the visitor must have courier orders.

Figure 7-3 provides an overview of the international visit program within DOD. At any time, participating activities have immediate access to all visit request status information.

Figure 7-3
International Visit Program



A request of visit authorization is not required at a contractor facility when the information to be disclosed is unclassified and (1) it is not subject to export controls, or (2) it is subject to export controls, but a contractor has an export license. It is not required at a DOD facility when the facility is open to the public and the information is open for public release according to service regulations.

However, if classified information is to be disclosed, a visit request must be submitted even though the contractor has a valid export authorization or license. In this case, the visit request is used to pass the security assurance on the visitors. Requests for classified documentary information resulting from a foreign visit shall otherwise be processed through normal foreign disclosure channels. In either case classified documentary information shall be transferred through government-to-government channels, unless the visitor is also acting as a courier and has courier orders.

Role of Security Cooperation Offices in International Visits

The security cooperation offices (SCOs) personnel should be cognizant of the official travel of both host nation personnel to DOD organizations, as well as the travel of DOD personnel into country. SCOs frequently coordinate visits by host nation personnel to destinations such as a geographic combatant command headquarters or a MILDEP installation for a program management review. However, the SCO cannot submit the visits request, which must originate in the host nation embassy in Washington DC through the FVS. SCOs must remind their host nation counterparts of this requirement and note that their own assistance in scheduling a visit is dependent on formal approval through the FVS. A SCO cannot approve a visit to any DOD organization or facility, other than its own office.

For DOD visitors traveling into the host nation, the SCO should control these through the granting or denying of country clearance. In doing this, the SCO follows the procedures in DOD 4500.54, *DOD Foreign Clearance Guide*. The SCO may also support DOD visitors by passing assurances and other documentation to and from the host nation, and by using its office as necessary to store CMI or CUI.

Defense Personnel Exchange Program

The Defense Personnel Exchange Program (DPEP) authorizes the exchange of personnel between the US military services and their counterparts of friendly governments for assignment to established positions within their force structure. This exchange is implemented under an agreement conforming to DODD 5530.3, *International Agreements*. Assignments can be negotiated as a reciprocal exchange of military personnel. Also, civilian position assignments such as intelligence analysts, scientists and engineers, medical personnel, and administrative specialists may be negotiated. Exchange personnel perform the functions of the specific position within the organization to which they are assigned. Since

they are not designated officials of their government, classified information may not be released into their permanent custody. They may only be given oral or visual access to specific classified information authorized in the applicable delegation of disclosure letter (DDL). Written procedures must be developed to prevent inadvertent disclosure of classified or CUI as described in DODD 5230.20. Such personnel may not be given access to information classified under the Atomic Energy Act of 1954, as amended. DPEP assignees may not act as a representative of their government or the USG.

Foreign Attendance at Classified Meetings Leading to Contract Opportunities

The USG has entered into cooperative agreements with allies and other friendly nations that allow the exchange of information in specific areas of mutual interest required for their participation in contractual opportunities. See chapter 13 of this textbook, "Systems Acquisition and International Armaments Cooperation Programs," for a discussion of reciprocal procurement memoranda of understanding. Planning for meetings that may lead to contracts for foreign nationals shall be based on the assumption that there will be foreign attendance. DODD 5200.12, *Conduct of Classified Meetings*, contains policies and procedures for sponsoring and conducting meetings involving classified information attended by foreign nationals.

Visits Overseas by Department of Defense Personnel

The policy for overseas travel of DOD personnel is covered under DODD 4500.54, *Official Temporary Duty Travel Abroad*, and DOD 4500.54-G, *Foreign Clearance Guide* (FCG). DOD components must appoint a responsible official and follow the FCG. Normally thirty days advance notice is needed before travel. Procedures also must be established to ensure disclosure authorization has been obtained if classified or export controlled unclassified information is to be divulged. A "theater clearance" is required for visits to a US military facility overseas as specified in the FCG. A "country clearance" is required for visits to a host government organization or contractor facility for classified discussions.

International Transfers

United States Classified Contracts with Foreign Firms

A USG agency may award or permit one of its contractors to award a classified contract to a foreign contractor, only if the classified information involved has been approved for release or is determined to be releasable to the government of that country under the NDP. In addition, the foreign government concerned must have entered into a security agreement with the US under which it agrees to protect US classified information released to it. User agency responsibilities are contained in DOD 5220.22-R, *Industrial Security Regulation*.

Transmission of Classified Materiel to Foreign Governments

Transmission of classified materiel to foreign governments, either to addresses in the US or outside the US, must be on a government-to-government basis, e.g., US Postal Service registered mail through an Army or Air Force APO or Navy FPO postal service; and such transmissions should be in accordance with DOD 5200.01, *DOD Information Security Program*, chapter VIII. Disclosures or denials are recorded in the SPAN. To assure compliance, each contract agreement, LOA, or other arrangement that involves the release of classified materiel to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by the appropriate DOD security and transportation officials and applicable foreign governments prior to release of the materiel. Government arrangements cannot be used as a means to bypass the ITAR. More information about the transfer of classified items may be found in chapter 11 of this textbook, "Foreign Military Sales Transportation Policy"

Defense Security Service Role in International Programs

A role of the Defense Security Service (DSS) is to provide government contracting agencies with an assurance that US defense contractors are both eligible to access and properly safeguard any classified information. In fulfilling this obligation, DSS administers the National Industrial Security Program (NISP) operating on behalf of the Under Secretary of Defense for Intelligence [USD (I)]. DSS does not develop industrial security policy. DSS implements industrial security policy established by USD (I) for international programs established by the Under Secretary of Defense for Policy [USD (P)].

Facility Security Clearance

Prior to a defense contractor being granted access to classified information, the contractor must be sponsored for a facility security clearance (FSC). This sponsorship is based upon a *bona fide* procurement need, and is submitted to DSS by an US or foreign government contracting activity or by another contractor already cleared under the NISP. DSS will conduct a facility clearance survey to determine the contractor's eligibility for access to classified information, and will review the contractor's organizational structure and key management personnel, and adjudicate any existing foreign ownership, control, or influence (FOCI). Once a favorable determination is made and a facility clearance is granted, the contractor will execute a security agreement with the USG. The security agreement is a legal contract to abide by the DOD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM). The NISPOM is a contractually binding document and mandates industrial security practices for contractors. The NISPOM derives its authority from the ITAR and implements applicable statutes, executive orders, national directives, and international treaties toward the protection of classified information.

The DSS verifies the export of classified articles and technical data against the license or the US company's empowered official's certification, assures that secure means of transfer have been arranged, and endorses the license back to the DOS. DSS oversees plant visits by foreign nationals and ensures that companies have adequate technology control plans in place for long-term foreign national visitors, foreign national employees, and for FOCI situations. DSS ensures appropriate transportation plans are in place for commercial overseas shipments of classified material and approves contractor international hand carriage arrangements. Additionally, DSS provides security assurances to other governments for US contractor facilities and personnel and obtains assurances on foreign facilities and personnel. It advises cleared contractors concerning program protection plans, ensures compliance, and trains DOD and contractor personnel on program protection planning. The DSS provides support to cleared contractors operating overseas, and monitors their compliance with the NISPOM. Finally, DSS provides counterintelligence (CI) support to cleared contractors, including CI awareness briefings. More information about DSS can be found at its website: http://www.dss.mil.

Technology Control Plan

The technology control plan (TCP) provides guidance on the control of access to classified and unclassified export controlled information by foreign employees and long-term foreign national visitors of a cleared US contractor's facility. The TCP explains how the requirements of the ITAR, the EAR, and the NISPOM will be carried out. The TCP is developed by the US contractor, based on the requirements of the ITAR, section 126.13c, and the NISPOM. The content regarding information access and restrictions may be derived from other documents provided by the USG (for example, the license provisos and the program security instructions or the form DD 254). The DSS will assist the contractor in developing the TCP and will approve it. A specific TCP may not be required if the company's internal security operating procedures, e.g., standard practice procedures (SPP) contain the necessary details. If security requirements are partially contained in a document such as an SPP and additional export control procedures are in a TCP, the latter must refer to the applicable portions of the other document.

Defense Industrial Security Clearance Office (DISCO)

The Defense Industrial Security Program (DISP) establishes procedures for safeguarding classified defense information which is entrusted to contractors. Included in these procedures is a system for determining the eligibility of industrial personnel for access to classified defense information. The Defense Industrial Security Clearance Office (DISCO) is a Central Adjudication Facility (CAF) responsible, on behalf of the Department of Defense (DOD) and twenty-three other departments and agencies for:

- Determining the personnel clearance eligibility of employees for access to classified information, foreign or domestic
- Maintenance of personnel clearance records and furnishing information to authorized activities
- Processing security assurances, clearances and visits involving the United States and foreign countries
- Monitoring the contractor's continued eligibility in the NISP

Foreign Government and North Atlantic Treaty Organization Information

Foreign Government Information

Foreign government information (FGI) is information that has been provided by a foreign government or international organization, or jointly produced, with the expectation that the information will be treated "in confidence." The information may be classified or unclassified. In addition to TOP SECRET, SECRET, and CONFIDENTIAL, many foreign governments have a fourth level of security classification, RESTRICTED as well as CUI that is provided in confidence.

As a result of numerous international security and program agreements, the NATO security agreement obligates member nations to adopt common standards of protection. US national policy affords FGI a degree of protection equivalent to that provided to it by the originating government or international organization. Since foreign government accountability and control measures often exceed those of the US, the US applies separate security procedures to protect FGI. Because most exchanges are with NATO and its members, the NATO standards are used as the baseline for U. S. procedures for protecting FGI.

FGI, including RESTRICTED and foreign government CUI, must be classified under E.O. 13526 in order to receive protection equivalent to that provided by the originating government or organization, as stipulated in E.O. 13526 and international agreements. FGI that is classified by the originating government or organization will be marked with the equivalent US classification, if it is not already marked in English, and the identity of the originating government or organization. Foreign government RESTRICTED and CUI are to be marked, "Handle as CONFIDENTIAL–Modified Handling Authorized." FGI cannot be provided to third country entities or used for a purpose other than that for which it was provided without the consent of the originating government or organization. It must receive protection commensurate with that provided by the originating government or organization. The procedures for handling FGI are contained in two national policy documents, E.O.13526, the presidential directive on safeguarding classified national security information, and DOD 5200.01.

Basic handling procedures for FGI are as follows:

- Storage. The same as US information of the same classification, but FGI is to be stored separately. FGI that is marked "Handle as CONFIDENTIAL–Modified Handling Authorized" is stored in the same manner as U. S. CUI, e.g., in a locked desk or file cabinet.

- Access. Using the need-to-know principle, no access by third country persons without the prior consent of the originating country or organization.
- Transmission. The same as US classified information of the same classification level; however, express commercial carriers cannot be used. Receipts are required for international transfers wherever they occur, although exceptions are made for RESTRICTED information. There are no receipts for CUI.
- Records. TOP SECRET–receipt, dispatch, internal distribution, annual inventory, and destruction (two persons); SECRET–receipt, dispatch, internal distribution, and destruction; CONFIDENTIAL–receipt and dispatch, and as required by originator

North Atlantic Treaty Organization Disclosure Security Procedures

Basic security requirements are necessary to comply with the procedures established by the US Security Authority for the North Atlantic Treaty Organization (USSAN) for safeguarding NATO information involved in international programs. DODD 5100.55 *USSAN Affairs* contains the terms of reference designating the Secretary of Defense as the USSAN for the USG. These requirements are consistent with USSAN Instruction 1-70 and implemented by DODD 5100.55, DOD C-5220.29, and the NISPOM. The foregoing documents must be consulted for specific details.

Classification Levels

NATO security regulations prescribe four levels of security classification, COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). The terms COSMIC and NATO indicate that the material is the property of NATO. Another marking, ATOMAL, is applied to US RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom atomic information that have been released to NATO. Once disclosed to NATO, the classified information losses its country of origin identity and is marked as NATO information. Thereafter, access, dissemination, and safeguarding of the information is accomplished in accordance with NATO procedures. The information remains the property of the entity that originated or furnished it.

Access Requirements

DOD and contractor employees may have access to NATO classified information only when access is required in support of a US or NATO program that requires such access, i.e., need-to-know.

Access to NATO classified information requires a final DOD personnel clearance (except for RESTRICTED) at the equivalent level and a NATO-specific security briefing discussed later in this chapter. A personnel security clearance is not required for access to NATO RESTRICTED information.

Foreign nationals from nations not members of NATO may have access to NATO classified information only with the consent of the originating NATO member nation or civil or military body. Requests with complete justification, as described in the NISPOM, will be submitted through the cognizant security office (CSO).

Disclosure Briefings

Prior to having access to NATO classified information, contractor and government personnel must be provided a NATO security briefing. The contractor's facilities security officer (FSO) will initially be briefed by the CSO. Annual refresher briefings will be conducted. When access to NATO classified information is no longer required, personnel will be debriefed, as applicable, and acknowledge their responsibility for safeguarding the NATO information.

Marking and Handling Disclosure Documents

Normally, NATO documents do not carry portion markings as are required for US classified documents. Nevertheless, all classified documents created by US contractors and DOD components will be portion-marked.

NATO classified documents, and NATO information in other documents, may not be declassified or downgraded without the prior written consent of the originating NATO member nation civil or military body. Recommendations concerning the declassification or downgrading of NATO classified information are to be forwarded to the central US registry (CUSR) via the CSO by contractors and via command or organizational channels by government personnel.

NATO classified documents, except for NATO RESTRICTED, are to be stored as prescribed in DODD 5100.55 and the NISPOM for US documents of an equivalent classification level. However, NATO documents must not be comingled with US or other documents. NATO restricted documents may be stored in locking filing cabinets, book cases, desks, other similar locked containers that will deter unauthorized access, or in a locked room to which access is controlled.

International Transmission of Classified Disclosure Documents

NATO policy requires the establishment of a central registry for the control of the receipt and distribution of NATO documents within each NATO member country. The CUSR, located in Washington, DC, establishes sub-registries at USG organizations for further distribution and control of NATO documents. Sub-registries may establish control points and sub-control points as needed within their activities for distribution and control of NATO documents. COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents must be transferred through the registry system.

Marking the Documents

When a document containing US classified information is being specifically prepared for NATO, the appropriate NATO classification markings will be applied to the document only after the US information contained in the document is authorized for release to NATO. If the information is to be provided pursuant to a NATO contract, the requirements of the NATO security aspects letter and security requirements checklist will be followed. However, if US classification guidance for the US information is not consistent with NATO classification guidance, the matter must be forwarded to the CSO for resolution.

Multinational Industrial Security Working Group Documents

The multinational industrial security working group (MISWG) is composed of the NATO countries, less Iceland, plus Austria, Sweden, Switzerland and Finland. It is an ad hoc group organized to rationalize different security practices and develop standard procedures for multinational programs. Although initially developed to standardize procedures among NATO member nations working jointly on a non-NATO project, the MISWG documents contain procedures that may be used in any bilateral or multilateral program or project, including NATO projects. NATO, NATO countries, and other countries have adopted the MISWG procedures. Therefore, they should be used as the baseline in preparing individual arrangements or when consolidated in a program security instruction (PSI), MISWG Document 5, for international programs.

Most of the MISWG documents provide procedural guidance for implementing security requirements for international programs. Other MISWG documents are used in preparing the content of international agreements and contracts involving access to classified information. The DSS may approve the use of the documents in individual commercial programs. However, the Designated Security Authority, DUSD (PI&CoS), will approve the use of the documents when they are required by an international agreement such as in a PSI.

More information on the MISWG Documents can be found in chapter 9 of the *International Programs Security Handbook*.

Committee on Foreign Investment in the United States and Foreign Ownership, Control or Influence

Committee on Foreign Investment in the United States (CFIUS)

The Exon-Florio Amendment to the Omnibus Trade and Competitiveness Act of 1988, as amended by the Defense Authorization Act for Fiscal Year 1993, empowers the President to suspend, prohibit or dissolve ("block") foreign acquisitions, mergers and takeovers of US companies. The President has broad authority to block a transaction under the statute if he determines the foreign interest acquiring control might take action that threatens to impair the national security. To exercise his authority, the President must find that:

- There is credible evidence that leads him to believe that a foreign interest might take action to threaten or impair national security
- Provisions of law, other than Exon-Florio and the Emergency Economics Powers Act, are not adequate to protect the national security

There is no mandatory requirement for a company to report under the law. Nevertheless, the President or his designee may investigate a merger, acquisition, or takeover at any time, including after a transaction has been concluded. The President can reopen a case on the basis of material omissions or material misstatements in the original notice.

The President delegated responsibility for carrying out the requirements of Exon-Florio to the interagency CFIUS. The CFIUS is comprised of representatives of the Departments of Treasury (chair), Defense, State, Energy, Homeland Security, Commerce, the US Trade Rep, Office of Science and Technology Policy, and the Attorney General. Membership may also include the heads of any other executive department, agency, or office as the President determines appropriate on a case-by-case basis.

Once CFIUS considers a possible transaction as the result of a notification by the investors, on its own initiative, or at the request of a third party, it has thirty days to decide whether to initiate an investigation. The investigation must be completed no later than forty-five days after its commencement, at which time the committee must present a recommendation to the President. The President is required to render a decision within fifteen days after completion of the investigation. If the President decides to take action as the result of a CFIUS investigation, he must submit a written report to Congress on the actions that he intends to take, including detailed rationale for his findings. The Committee or a lead agency of the Committee may, on behalf of the Committee, negotiate, enter into or impose and enforce any agreement or condition with any party to the specified transaction in order to mitigate any threat to the national security of the US that may arise as a result of the transaction.

Foreign Ownership, Control or Influence (FOCI)

It is not in the interest of the US to permit foreign investment in the defense industrial base where it is inconsistent with US national security interests. USG contracts requiring access to classified information may be awarded to companies under FOCI when adequate safeguards exist to protect national security interests. Within the context of the DOD, national security interests are represented by information and technical data inherent in the development and production of military systems, such as system capabilities and vulnerabilities. If this knowledge is lost or compromised, potential adversaries of the US would have the capability to duplicate or neutralize those systems. As a result, the US must take steps to ensure that foreign interests do not have the power to direct or decide matters for a company operating under a facility security clearance if such power may result in the

unauthorized disclosure of classified and CUI, or may adversely affect the award or performance of classified contracts. FOCI encompasses the possible avenues from which unauthorized foreign power may be exerted. When competent authority determines foreign interests have the power to exert such power, measures must be established to negate the FOCI or mitigate the associated risk.

When a company performing classified work is to be acquired by or merged with a foreign interest, an industrial security review is undertaken. The purpose of the review is to determine whether existing industrial security measures require enhancement. The matter of FOCI is considered in the aggregate, and the fact that FOCI elements are present will not necessarily bar a company from receiving a facility security clearance. There are many components of foreign involvement requiring examination to determine whether a company is under FOCI and the extent of FOCI, such as those identified on Standard Form (SF) 328. Documents other than the SF 328 are analyzed, to include filings with the Security and Exchange Commission for publicly traded companies, articles of incorporation, by-laws, loan and shareholder agreements, and other documents pertinent to potential foreign control or influence.

The FOCI is then examined within the context of risk factors such as the foreign intelligence threat, potential for unauthorized technology transfer, record of compliance with laws, regulations, and contracts, and the nature of applicable international agreements between the US and foreign governments. If a company is determined to be under FOCI, and risks associated with FOCI are considered unacceptable, the company would be ineligible for a facility clearance or an existing clearance would be suspended or revoked, unless steps are taken to negate FOCI or mitigate associated risks to the satisfaction of the USG. The principal objective of each arrangement is to ensure there is no unauthorized access to classified and CUI by foreign owners, their agents or representatives, or by other non-ownership derived sources of foreign control or influence. For a detailed discussion of these arrangements and agreements, refer to the *International Programs Security Handbook* and the NISPOM.

Summary

The DOD has identified the areas where US-origin technology and other sensitive information should be rigidly protected. These include the critical military technology products, transfer mechanisms and information which DOD has determined should be subject to export and disclosure controls. The NDP provides guidance on the disclosure and release of US classified military information. The criteria for disclosure decisions in the NDP-1 and NSDM 119 do not categorically dictate whether classified military information will be released to a specific country. These decisions are made on a case-by-case basis, in accordance with satisfying all of the five policy objectives of NSDM 119, which are restated in DODD 5230.11.

Controlling the transfer of selected technologies is but one way to maintain the integrity of the US defense-related industrial base. However, the extent of control is at issue. Many feel that controls should be tempered by the realities associated with worldwide competition and the impacts upon US industry and the preservation of US economic security as the prerequisite condition to maintaining national security. Others, however, as noted in the chapter introduction, believe that transfer of advanced technology for military or dual-use applications can lead to the proliferation of dual-use technology as well as of nuclear and conventional arms. Technology transfer issues continue to play an important role in government-to-government sales programs, commercial sales programs, international armaments cooperation programs, and industrial base considerations.

Policies and supporting directives governing technology transfer emphasize the application of the US policy and legal requirements in the AECA, E.O.13526, NSDM 119, NDP-1, and DODD 5230.11 to each case, and the analysis of a potential recipient's need, the intended use and protection measures for such information. The directives are explicit as to procedure and channels to be followed to preclude unwarranted release and disclosure of information.

References

Laws

Arms Export Control Act

Atomic Energy Act of 1954

Defense Authorization Act of 1986 (Nunn Amendment/NATO Cooperative R&D)

Defense Authorization Act of 1993, Defense Technology and Industrial Base Reinvestment and Concession

Energy Reorganization Act of 1974

Export Administration Act of 1979

Public Law (PL-110-49), 26 July 2007, Foreign Investment and National Security Act of 2007.

Stephenson-Wydler Technology Innovation Act of 1980

Department of State Documents

International Traffic and Arms Regulations (ITAR) (22 CFR 120-130).

Website: http://www.pmdtc.gov

Department of Defense Documents

DOD 5105.38-M, *Security Assistance Management Manual* (SAMM), chapter 3.

DODD 2040.2, *International Transfers of Technology, Goods, Services and Munitions*.

DOD 5220.22-M, *National Industrial Security Programs Operating Manual* (NISPOM).

DOD 5220.22-R, *Industrial Security Regulation*.

DODD 5230.11, *National Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations*.

DODD 5230.20, *Visits and Assignments of Foreign Nationals*.

DODD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*.

DOD 5200.01, *DOD Information Security Program*.

DOD 4500.54-G, *DOD Foreign Clearance Guide*.

DODD 5200.12, *Conduct of Classified Material*.

DODI 5200.21, *Dissemination of DOD Technical Information*.

DODD 5230.24, *Distribution Statements on Technical Documents*.

DODD 5230.9, *Clearance of DOD Information for Public Release*.

DODD 5400.07, *Freedom of Information Program*.

US Security Authority for the North Atlantic Treaty Organization, Instruction I-07.

Other US Government Documents

Executive Order 13526.

National Security Decision Memorandum 119.

National Industrial Security Program Operating Manual (NISPOM).

Website: www.dtic.mil/whs/directives/corres/html/52202m.htm

Other

International Programs Security Handbook. Website: www.avanco.com/ips_handbook.html

Attachment 7-1
International Programs Security Training Memorandum

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1010
22 OCTOBER 1999

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN, JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES

Subject: Training in International Security and Foreign Disclosure Support to International Programs

Strong allies, and well-equipped coalition partners, make America stronger. It is, therefore, in America's national security interest to promote cooperation with other nations, seek-international participation in our weapons acquisition process and support appropriate foreign military sales.
At the same time, we must ensure that sensitive and classified US technology and military capabilities are protected. Classified information should be shared with other nations only when there is a clearly defined advantage to the US Disclosures must be carefully designed to achieve their purpose, and recipients must protect the information. To make certain that we accomplish these goals, certain security arrangements must be in place prior to any foreign participation in DOD programs. It is therefore vital that every DOD employee involved in international programs understand these security arrangements, as well as the laws, policies, and procedures that govern foreign involvement in our programs.

To ensure that all relevant employees are fully trained in this area, the Office of the Deputy to the Under Secretary of Defense (Policy) for Policy Support DUSD(PS)) has developed a course of instruction that covers the practical application of relevant law, executive orders, and DOD policies on this subject. All DOD personnel responsible for negotiating, overseeing, managing, executing or otherwise participating in international activities shall successfully complete either the International Security Requirements Course offer by DUSD(PS), the International Programs Security and Technology Transfer Course taught by the Defense Systems Management College, or an executive version of the course for mid-level and senior managers not being developed. This requirement applies to anyone who works in an office dealing exclusively with international matters, in international cooperation offices within broader functional offices, and those working on international issues with a DOD program. Examples of applicable activities include: security assistance, cooperative research, foreign disclosure, specific country relationships, and other international policy activities.

The law also requires that we consider systems of allied nations, or the co-development of systems with allied nations, before a US-only program may be initiated. Therefore, the basic, intermediate, and advanced program manager courses at DSMC shall include at least four hours of training in international security requirements related to acquisition programs. Anyone working in program offices where any international activities occur, including exports, must also complete the full five day course. DOD personnel who are newly assigned to international programs shall participate in one of the courses within six months of the assignment.

To ensure consistency, DOD components that offer specialized training in foreign disclosure and security requirements for international programs shall coordinate the contents of their courses with the DUSD(PS).

//SIGNED//
John J. Hamre

Attachment 7-2
National Disclosure Policy Committee Members

National Disclosure Policy Committee Members

The General Members are representatives of:

The Secretary of State

The Secretary of Defense (appoints Chairman)

The Secretary of the Army

The Secretary of the Navy

The Secretary of the Air Force

The Chairman, Joint Chiefs of Staff

The Special Members are representatives of:

The Secretary of Energy

The Director of National Intelligence

The Under Secretary of Defense for Policy

The Under Secretary of Defense for Acquisition, Technology and Logistics

The Under Secretary of Defense for Intelligence

The Assistant Secretary of Defense for Networks and Information Integration

The Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

The Director, Defense Intelligence Agency

The Director, Missile Defense Agency

The Director, National Geospatial-Intelligence Agency

The Director, National Security Agency